Contract No:

This document was prepared in conjunction with work accomplished under Contract No. 89303321CEM000080 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Effect of GPS Manipulation to Traditional and Next Generation Relay Protection

Project Start and End Dates
Project Start Date: 10/1/2019
Project End Date: 9/30/2021

Project Highlight
This project's objective is to test the effect of GPS timing variations on relay protection algorithms to determine vulnerabilities and the associated hazards to the electric grid. This will focus on traveling wave protection which detects wave propagation down a line from a fault and can detect the location of the fault to the specific tower.

Project Team
Principal Investigator: Klaehn Burkes
Team Members: Ian Webb, Sean Krautheim
External Collaborators: Johan Enslin, Moazzam Nazir (Clemson University)

Abstract
This project's objective is to test the effect of GPS timing variations on relay protection algorithms to determine vulnerabilities and the associated hazards to the electric grid. This will focus on time domain protection which utilizes traveling waves measured on the transmission lines to detect the fault within a tower span. This requires the use of GPS to sync the two substations and can be vulnerable to GPS manipulation. However, the effects of GPS manipulation are not a commonly known risk. Therefore, this LDRD will address the risks of GPS manipulation for on a new protective relay technology that has the potential to change protective relaying. For time domain protection a GPS resilient architecture was implemented and tested for time domain protective relays through a direct serial fiber connection between the two relays. This allows for one relay to be the master and provide synchronization outside of timestamp for traveling wave protection.

Objectives
- Set up SEL-T400L traveling wave protection relay within the SRNL-Critical Infrastructure, ICS and Cybersecurity (S-CIIC) lab
- Program protective relays to perform time domain protection through controller hardware in the loop platform RSCAD.
- Time shift IRIG-B to perform time manipulation and then conduct faulting sequences on controller hardware in the loop test bed.
- Develop best practice for implementing traveling wave protection relay under GPS manipulation.

REVIEWS AND APPROVALS

1. Authors:

Klaehn Burkes _____

Ian Webb _____

Sean Krautheim _____

Signature Date

2. Technical Review:

_____

Name and Signature Date

3. PI's Manager Signature:

_____

Name and Signature Date

4. Intellectual Property Review:

This report has been reviewed by SRNL Legal Counsel for intellectual property considerations and is approved to be publicly published in its current form.

SRNL Legal Signature

_____

Name and Signature

Introduction

Modern electric power systems are undergoing structural changes. Systems are upgrading supervisory control and data acquisition (SCADA) systems and replacing electromechanical protective relaying equipment with modern microprocessor-based relays. These advancements have allowed for more precise control through distributed and real time methods, though requiring more communication between intelligent electronic devices (IEDs) and remote terminal units (RTUs). These new devices are, at their core, programable logic controllers (PLCs) that resemble the communication protocols of industrial control systems (ICS) [1]. To complement these changes, the protocols and communication methods specific to the electric power system (traditionally Distribution Network Protocol (DNP3)) are being replaced with International Electrotechnical Commission (IEC) standard 61850. DNP3 has no timestamped data in its messaging protocol, meaning relay protection algorithms are not affected by GPS time stamps or data [2]. Contrarily, IEC 61850 uses many different protocols that are based on fast fiber connections that utilize timing as a key part of the data transfer. These protocols, such as Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Event (GOOSE), and Sample Measured Values (SMV), all run over Transmission Control Protocol/Internet Protocol (TCP/IP) networks utilizing high speed switching ethernet. TCP/IP connections enable IEC 61850 to obtain the necessary response times to achieve millisecond protective relaying controls [3]. Therefore, the future of protective relaying is relying on accurate and synchronized timing to improve the electric power system reliability and stability.

An example of a protection scheme utilizing high-speed communication is traveling wave protection. This protection scheme monitors one end of a transmission line for different wave propagation from a fault. Another relay monitors wave propagation from a fault in another substation at the other end of the transmission line. These two can then determine where the fault is located up to the specific tower the fault occurs on. This calculation requires two substations to be synchronized on an accurate clocking signal, typically a GPS receiver. Figure 1 represents this electrical system architecture.

This project's objective is to research the effects of GPS signal manipulation between two substations. Manipulation was performed by slowly walking off one substation's GPS signal and monitoring the protection algorithms to determine the failure mechanisms of these millisecond protective relaying functions. SRNL has already proven in previous work that the GPS receivers cannot detect small steps of GPS signal deviations; this implies that a GPS attack does not cause the receiver to revert to a holdover posture. Also, SRNL proved that line differential protection was not affected by GPS walk off due to the requirement to have one relay operate as a master clock. This project will allow for SRNL to become a leader in the field of GPS timing manipulation with previous knowledge of GPS receiver operation and the knowledge gained through determining the failure mechanisms of the millisecond protective relay functions of differential and time domain protection.

Approach

The approach for implementing and testing this is through setting up a controller hardware in the loop (CHIL) test bed for the protective relays. CHIL testing allows for controllable and repeatable testing of a variety of electronic power grid components, including protective relays. This allows for running many different power grid simulations and connecting the signals from within the simulation to get precise controlled results.

These simulations were produced via the software RSCAD, running on an RTDS stack. These systems allow precise emulation of an electrical power grid that can output current waveforms consistent with that emulation, including waveforms for fault currents. These outputs would be passed at a low level to the protective relay, which would interpret the signals to correspond to a "real" power system scenario via appropriate gain settings. The simulation used in this set of experiments consisted of varying lengths of transmission line between two simulated power generation plants, with the protective relays situated at either end of a 100 mile transmission line between the generation plants, as shown in Figure 3. RSCAD/RTDS additionally utilized digital inputs from the protective relays to take contactor inputs to control the virtual breakers within the simulation.

To implement a traveling wave protection scheme, including precise timing signals and appropriately spoofed GPS signals, the TyphoonHIL system simulated IRIG-B time code outputs to supply to the protective relays. TyphoonHIL then added time delay to one time code to simulate a GPS signal manipulation. This would internally cause one relay's high precision time measurement to be the delay was added in TyphoonHIL.

Error! Reference source not found. represents the actual test network established in the S-CIIC, consistent with this design.

Through combining the two technologies (RSCAD/RTDS and TyphoonHIL), every input and output to the protective relays were controlled by the operator to test the protective relay with values consistent with values commonly found during in-field deployment. The emulation scenario further allowed for flexible implementation and testing of multiple differential protection architectures to examining their vulnerabilities to GPS time walk off; specifically, those vulnerabilities directly related to the different IRIG-B inputs for the relays.

Accomplishments

- ✓ Implemented and tested a GPS resilient architecture for traveling wave protective relays through a direct serial fiber connection between the two relays.
- ✓ Established a relay experimental test bed to function test relays with controllable voltage and current outputs, timing signals, and breaker inputs
- ✓ Demonstrated that traveling wave protective relay algorithm can be resilient to GPS manipulation
- ✓ Traveling wave protection relay tripped faster than differential protection relay even under the presence of GPS manipulation.
- ✓ Developing Journal Publication on Results

Future Directions

- Present findings to DoD sponsors interested in classified simulation capability's
- Establish a classified grid simulation system at SRNL

FY 2021 Peer-reviewed/Non-peer reviewed Publications

1. I. Webb, K. Burkes, "Simulation and Testing of a GIC Protection Device on Transformer," Submitting to IEEE Transactions on Power Delivery.

Intellectual Property

None.

Total Number of Post-Doctoral Researchers
None.

Total Number of Student Researchers
Moazzam Nazir (Clemson University)

Images, Charts, and Figures

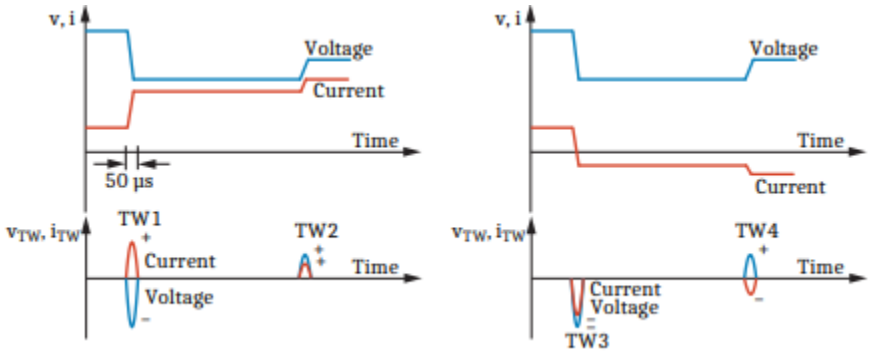

Figure 1. Traveling Wave Protection Operating Principle

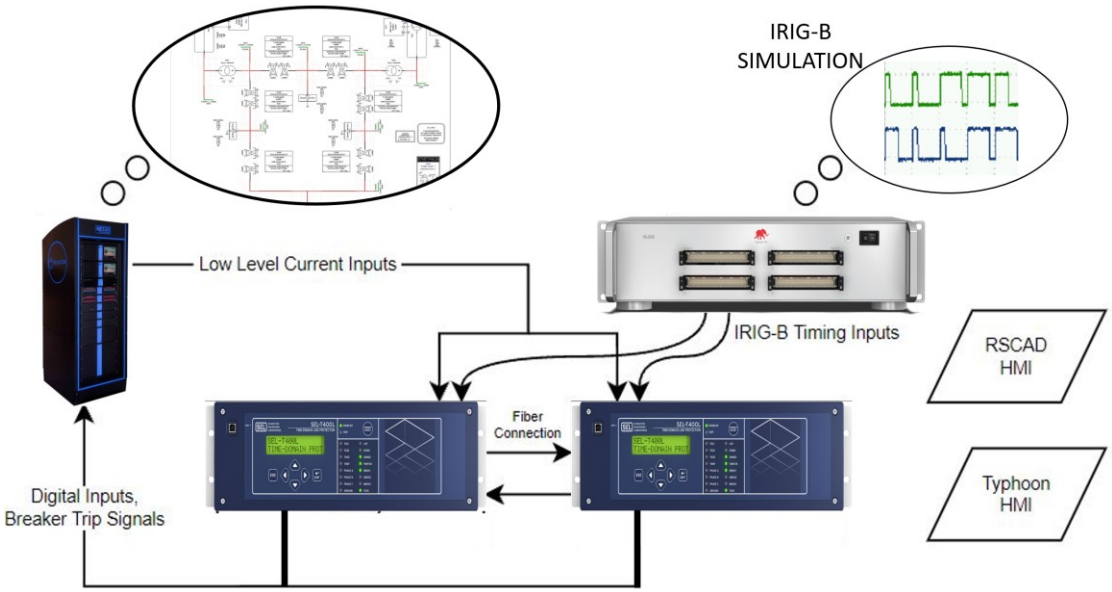

Figure 2. S-CIIC setup of relays, RTDS, and Typhoon

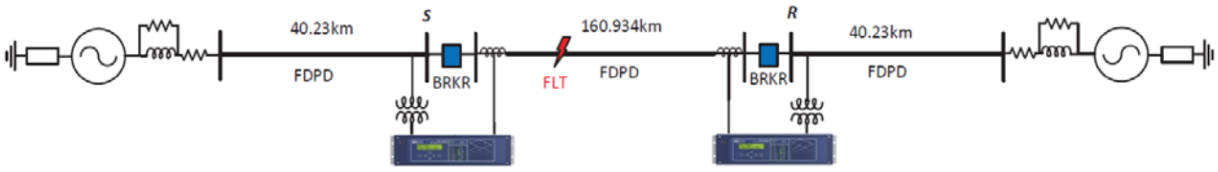

Figure 3. Diagram of Simulation

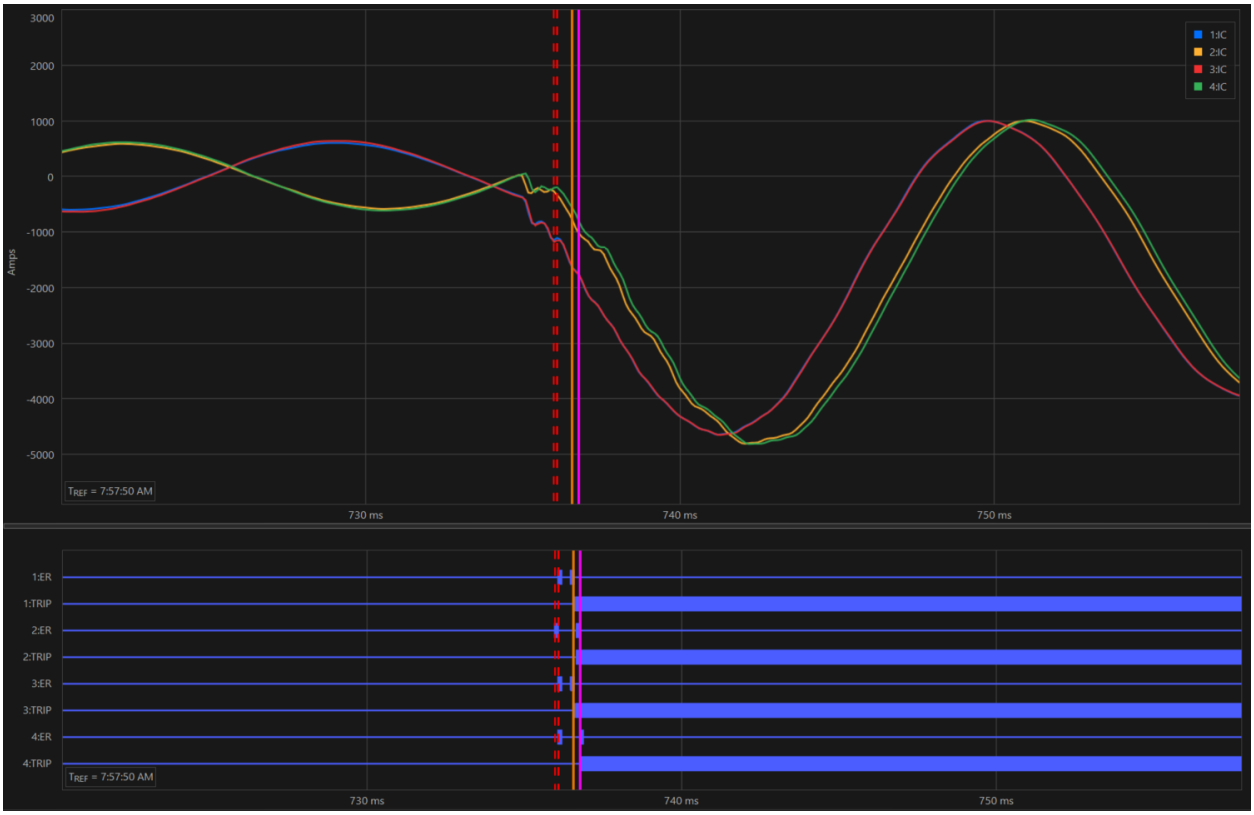

Figure 4. Fault Current at Sending and Receiving-End Relays with No Time Spoof and Time Spoof = +1ms (top), Relay TRIP Signal Assertions at Sending and Receiving End (bottom)

Works Cited

(1) S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, D. Holstein, J. Tengdin, K. Fodero, M. Simon, M. Carden, M. Yalla, T. Tibbals, V. Skendzic, S. Mix, R. Young, T. Sidhu, S. Klein and J. Weiss, "Cyber Security Issues for Protective Relays," GE Grid Solutions.

(2) S. East, J. Butts, M. Pap and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in *International Federation for Information Processing*, 2009.

(3) M. Gadelha da Silveira and P. Henrique Franco, "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," in *6th Annual PAC World Americas Conference*, Raleighm North Carolina, 2019.